区块链中矿池选择策略的研究与分析

邱　剑，吝伟华†

(华北电力大学 控制与计算机工程学院，河北 保定 071003)

摘　要：在基于工作量证明（proof of work, Pow）的区块链网络中，矿工通常选择加入矿池。由于存在多个矿池并且不同的矿池拥有的算力不同以及可能采取不同的奖励机制，所以矿工可以在不同的矿池中获得不同的收益。针对矿工面临的矿池选择问题，建立了一个基于风险决策准则的矿池选择模型，研究了矿池算力和奖励机制对矿工最优选择策略的影响。首先计算了矿工在不同矿池中的收益，给出收益矩阵；其次分别利用最大可能性准则和期望值准则得出最优选择策略；最后通过仿真实验，对提出的策略进行了验证分析。实验结果表明，提出的策略与简单策略相比，在绝大多数情况下能为矿工带来更高的收益。

关键词：比特币；区块链；矿池；奖励系统；风险决策

中图分类号：TP3　　doi: 10.19734/j.issn.1001-3695.2018.12.0875

Research and analysis of mining pool selection strategy in blockchain

Di Jian, Lin Weihua†

(*School of Control & Computer Engineering*, *North China Electric Power University*, *Baoding Hebei* 071003 , *China*)

Abstract: In a blockchain network based on Proof of work(Pow) , miners usually choose to join the mining pool. As there are many mining pools and different mining pools have different computing power and may adopt different reward mechanisms, miners can get different rewards in different mining pools. For the choice of mining pool faced by the miners, This paper proposed a mining pool selection model based on risk decision criteria, aiming at the problem of miners' selection of mining pools, and studied the effect of computing power and reward mechanism on the miners' optimal pool selection decisions. Firstly, calculated the miners' reward and given the reward matrix, Secondly, by using the maximum likelihood criterion and the expectation criterion respectively derived the optimal selection strategy, Finally, through simulation experiments, validated the proposed pool selection strategies. Experimental results show that compared with the simple strategy, the proposed strategy can bring higher rewards to the miners in most cases.

Key words: bitcoin; blockchain; mining pool; reward system; risk decision

0　引言

自从 2008 年中本聪发表比特币白皮书以来[1]，区块链技术受到了越来越多的关注，它的主要特性包括去中心化、去信任、集体维护、安全性和不可窜改性[2]。由于这些特性，区块链技术可以应用在众多领域，如金融、能源互联网、信息安全[3~6]等方面。比特币作为区块链技术的典型应用，比特币系统利用工作量证明的共识机制[7]实现交易的不可窜改性和不可伪造性。在比特币系统中，挖矿是指所有参与者通过贡献自己的算力解决一个难度可动态调整的数学问题，寻求一个符合条件的随机值产生新区块的过程，参与者叫做矿工。如果一个矿工成功发现了一个区块，那么他可以得到这个区块的奖励，作为贡献自己算力的报酬。挖矿难度会根据系统当前生成区块的难易自动调节，一般设置每十分钟左右产生一个区块。实际上，在当前比特币系统中，由于算力过于庞大，独立矿工想要发现新发现新区块的概率基本为零[8]。因此矿工通常会选择加入矿池来提高收益的稳定性，同时矿池可以采取任意的挖掘策略[9]。

矿池通常由一个管理员和多个矿工组成，无论矿池内的哪个矿工发现了新区块，那么新区块的奖励会按照矿工的贡献比例分配给矿池内的所有矿工。由于产生完整工作量证明十分困难，管理员通常会为每个矿工设定一个难度较低的数学问题，并要求矿工提交这个问题的解决方案，也就是一个满足条件的随机值，通常称这个解决方案为部分工作量证明。目前，矿池奖励分配系统[10]主要 Proportional、Pay-per-share(PPS)、Pay-per-last-N-shares (PPLNS) 有三种。前两者统称为简单方法。Proportional 方法的原理是当矿池发现新区块时，根据矿工对矿池付出的算力大小分配给其相应的收益。PPS 方法的原理与 Proportional 唯一的不同点是无论当前矿池有没有发现新区块，都会按矿工的贡献大小分发报酬。PPLNS 原理指在若干个回合后，将矿池所获得的奖励平均分配给最近提交的 N 个部分工作量证明。关于矿池选择策略有以下研究：文献[11]研究了算力和网络延迟两个因素对矿池选择策略的影响并建立了一个演化博弈模型来分析这些因素对矿池选择策略的影响；文献[12]研究了不同的奖励分配机制以及 PPLNS 机制中的 N 对矿工收益的影响。文献[12]只研究了独立矿池采取不同奖励分配系统对矿工收益的影响，而在现实情况中，在一个区块链网络中，通常存在多个具有竞争关系的矿池。在此基础上，本文研究了具有竞争关系的矿池算力以及不同奖励分配机制对矿池选择策略的影响，提出了一种矿池选择策略。

收稿日期：2018-12-03；**修回日期：**2019-02-15

作者简介：邱剑（1968-），男，高级工程师，河北保定人，主要研究方向为区块链、加密货币、信息安全；吝伟华（1993-），男（通信作者），硕士研究生，主要研究方向为区块链、智能合约（linwh01@126.com）.

1 矿池选择策略

在本章中，假设这样一种场景，在一个区块链网络中，全网算力为 1，且只存在两个矿池 A 和 B，它们均进行诚实挖掘，不发起任何攻击[13,14]。其中矿池 A 采取 Proportional 奖励分配系统且其算力为 α，矿池 B 采取 PPLNS 奖励系统，其算力为 β，则 $\alpha+\beta=1$。在 PPLNS 系统中，假设每个回合中有 M 个部分工作量证明，矿工提交的部分工作量证明在 M 中的位置是随机的，即概率为 $p_i=1/M$，在不同的回合中，部分工作量证明的位置也是随机的。同时，本文假设在每个回合中挖矿难度 D 和每发现一个区块的奖励 R 是固定不变的，每个回合持续时间 T 恒定不变；同时，在该文研究中，不考虑矿池收取的费用，即矿池将所获得的全部区块奖励分配给矿工。

1.1 矿池收益

通常来说，矿工拥有算力越大则发现新区块的概率越大。由文献[1]可知，挖掘区块的过程近似于泊松分布，在恒定的算力下，区块以一定的概率被独立开采。由文献[10]可知，一个算力为 H 的节点在 t 时间段内，挖到的区块数量为 $\frac{Ht}{2^{32}D}$，获得的期望收益为 $\frac{HtR}{2^{32}D}$。

由此可得，在 K 个回合中共包含 KT 个时间单位，则矿池 A 和矿池 B 在 KT 时间内挖到的区块数量分别为 $\frac{\alpha KT}{2^{32}D}$、$\frac{(1-\alpha)KT}{2^{32}D}$。在 K 个回合中，系统共会产生 K 个区块，总的区块奖励为 KR，则矿池 A 和矿池 B 分别获得的区块奖励为 αKR、$(1-\alpha)KR$。所以得到矿池 A 中每个部分工作量证明的奖励为

$$R_A=\frac{1}{M}\alpha KR \quad (1)$$

矿池 B 中每个部分工作量证明的奖励为的收益为

$$R_B=\frac{1}{N}(1-\alpha)KR \quad (2)$$

K 个回合共有 KM 个部分工作量证明。由文献[12]可知，令 $N=(k-1)M+j$，$k\in[1,K]$，$j\in[1,M]$，可以得到矿工的收益矩阵，如表 1 所示。

表 1 矿工收益矩阵 1

Table 1 Miner's reward matrix 1

状态	矿池 A	矿池 B	概率 P
s_1	$\frac{1}{M}\alpha KR$	$\frac{k-1}{N}(1-\alpha)KR$	$\frac{M-j}{M}$
s_2	$\frac{1}{M}\alpha KR$	$\frac{k}{N}(1-\alpha)KR$	$\frac{j}{M}$

令

$$R_{a,1}=R_{a,2}=\frac{1}{M}\alpha KR \quad (3)$$

$$R_{b,1}=\frac{k-1}{N}(1-\alpha)KR \quad (4)$$

$$R_{b,2}=\frac{k}{N}(1-\alpha)KR \quad (5)$$

$$r_{a,1}=r_{a,2}=\frac{1}{M}\alpha \quad (6)$$

$$r_{b,1}=\frac{k-1}{N}(1-\alpha) \quad (7)$$

$$r_{b,2}=\frac{k}{N}(1-\alpha) \quad (8)$$

其中：a,b 分别代表矿池 A、B；1、2 分别对应状态 s_1,s_2。

1.2 最大期望值准则

最大期望值准则的原理为：

假设各事件发生的概率为 p_j，采用第 i 种策略在发生第 j 事件下的益损值（即收益矩阵中代表“策略—事件”对的各元素）记为 a_{ij}，则各策略的期望收益为 $E=\sum_{j=1}^{n}p_j a_{ij}, i=1,2,\ldots m$。其中：m 指可采用的策略（方案个数）；n 指可能出现的事件（状态）个数，$\sum_{j=1}^{j=n}p_{j=1}$。决策标准为从这些期望收益值中选取最大者，其对应策略即为最优策略。

利用以上原理，分别令 $E(A)$、$E(B)$ 为矿工在矿池 A 和矿池 B 的期望收益值，由表 1 得

$$E(A)=\frac{1}{M}\alpha KR\cdot\frac{M-j}{M}+\frac{1}{M}\alpha KR\cdot\frac{j}{M}=\frac{1}{M}\alpha KR$$

$$E(B)=\frac{k-1}{N}(1-\alpha)KR\cdot\frac{M-j}{M}+\frac{k}{N}(1-\alpha)KR\cdot\frac{j}{M}=\frac{1}{M}(1-\alpha)KR$$

令 $R_E=\frac{E(A)}{E(B)}-1$，得 $R_E=\frac{2\alpha-1}{1-\alpha}$。

a)当 $0<\alpha<\frac{1}{2}$，$R_E<0$，$E(A)<E(B)$，则选择矿池 B。

b)当 $\frac{1}{2}<\alpha<1$，$R_E>0$，$E(A)>E(B)$，则选择矿池 A。

c)当 $\alpha=\frac{1}{2}$，$R_E=0$，$E(A)=E(B)$，显然，矿池 A 的方差为零，期望收益值更加稳定，即矿池 A 为最优策略。

1.3 最大可能性准则

1)矿工在每个回合中提交一个部分工作量证明

根据最大可能性准则，当 $\frac{M-j}{M}>\frac{j}{M}$ 时，即认为 $R_{b,1}$ 会发生。若 $R_{b,1}>R_{a,1}$，则选择矿池 B，否则选择矿池 A，

当 $\frac{j}{M}\geq\frac{M-j}{M}$ 时，若 $R_{b,2}>R_{a,2}$，则选择矿池 B，否则选择矿池 A；当 $\frac{M-j}{M}=\frac{j}{M}$ 时，矿池 A 和矿池 B 都为最优策略。

由此得：

定理 1 当 $1\leq j<\frac{M}{2}$ 时，若 $0<\alpha<\frac{1}{2}$，则当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}>1$ 时，池 A 为最优策略，当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}=1$ 时，池 A 与池 B 均为最优策略，当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}<1$ 时，池 B 为最优策略，若 $\frac{1}{2}<\alpha<1$，则最优策略为池 A。

当 $\frac{M}{2}\leq j\leq M$ 时，若 $0<\alpha<\frac{1}{2}$，则当池 B 为最优策略。若 $\frac{1}{2}<\alpha<1$，则当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}>1$ 时，最优策略为池 A，当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}<1$ 时，最优策略为池 B，当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}=1$ 时，池 A 与池 B 均为最优策略。

证明：

a)当 $\frac{M-j}{M}>\frac{j}{M}$ 时，即 $1\leq j<\frac{M}{2}$，令 $R_1=\frac{R_{a,1}}{R_{b,1}}-1=\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}-1$，当 $R_1>0$ 时，$R_{a,1}>R_{b,1}$，选择池 A。当 $R_1<0$ 时，$R_{b,1}>R_{a,1}$，选择池 B。当 $R_1=0$ 时，$R_{a,1}=R_{b,1}$，池 A 与池 B 均为最优策略。当

$\frac{1}{2}<\alpha<1$ 时，$R_1>0$ 恒成立，故选择池 A。当 $0<\alpha<\frac{1}{2}$ 时，需要进一步计算 R_1 的值，从而作出相应的选择。

b)当 $\frac{j}{M}\geq\frac{M-j}{M}$ 时，即 $\frac{M}{2}\leq j\leq M$ 令 $R_2=\frac{R_{a,2}}{R_{b,2}}-1=\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}-1$，若 $R_2>0$，则 $R_{a,2}>R_{b,2}$，选择池 A。若 $R_2<0$，则 $R_{b,2}>R_{a,2}$，选择池 B。若 $R_2=0$，则 $R_{a,2}=R_{b,2}$，池 A 与池 B 均为最优策略。当 $0<\alpha<\frac{1}{2}$ 时，显然 $R_2<0$，选择池 B。当 $\frac{1}{2}<\alpha<1$ 时，需进一步计算，从而作出相应的选择。接下来，通过举例来进一步阐明上文提出的选择策略是否有效。

令 M=4，K=2，$\alpha=0.45,\beta=0.55$，则 $N\in\{1,2,\ldots,8\}$，在每个回合中矿工所提交部分工作量证明的位置有四种情况，矿工获得的收益占矿池 B 总收益的比例如表 2 所示，不同 N 的情形下矿工状态的可能性大小以及矿工收益占比如表 3 所示。

表 2　不同 N 下的矿工收益占比

Table 2　Miner's reward share under different N

Case	Ⅰ	Ⅱ	Ⅲ	Ⅳ
N=1	0	0	0	1
N=2	0	0	1/2	1/2
N=3	0	1/3	1/3	1/3
N=4	1/4	1/4	1/4	1/4
N=5	1/5	1/5	1/5	2/5
N=6	1/6	1/6	2/6	2/6
N=7	1/7	2/7	2/7	2/7
N=8	2/8	2/8	2/8	2/8

表 3　不同状态时对应的矿工收益

Table 3　Miners' reward in different states

N	S	P	R
1	{ⅠⅡⅢ}	p_1=3/4	0
	{Ⅳ}	p_2=1/4	1
2	{ⅠⅡ}	p_1=1/2	0
	{Ⅲ Ⅳ}	p_2=1/2	1/2
3	{Ⅰ}	p_1=1/4	0
	{Ⅱ Ⅲ Ⅳ}	p_2=3/4	1/3
4	{Ⅰ Ⅱ Ⅲ Ⅳ}	p_2=4/4	1/4
5	{ⅠⅡⅢ}	p_1=3/4	1/5
	{Ⅳ}	p_2=1/4	2/5
6	{ⅠⅡ}	p_1=1/2	1/6
	{Ⅲ Ⅳ}	p_2=1/2	2/6
7	{Ⅰ}	p_1=1/4	1/7
	{Ⅱ Ⅲ Ⅳ}	p_2=3/4	2/7
8	{Ⅰ Ⅱ Ⅲ Ⅳ}	p_2=4/4	2/8

在给出矿池算力以及在不同 N 的情况下矿工的收益情况，如表 4 所示。

将 $\alpha=0.45$ 代入，可得，分别对应于 N={1,2,..,8}的最优策略为{A,B,B,B,A,B,B,B}。

2)矿工在每个回合中提交多个部分工作量证明

假设矿工在每个回合中可以提交多个部分工作量证明，为了简便起见，本文研究了矿工每个回合可以提交两个部分工作量证明，并且这两个部分工作量证明的位置是相邻的，使用最大可能性准则进行分析。由文献[12]得收益矩阵如表 5 所示。

根据最大可能性准则：

当 $1\leq j<\frac{M}{2}$ 时，$p_1>p_3>p_2$，选择状态 s_1

当 $j=\frac{M}{2}$ 时，$p_1=p_3>p_2$，状态 s_1 与 s_3 的概率相等，选择 s_3

当 $\frac{M}{2}<j\leq M$ 时，$p_3>p_1>p_2$，选择状态 s_3

表 4　不同 N 对应的最优选择策略

Table 4　Optimal selection strategy corresponding to different N

N	R_a	R_b
1	$R_{a,1}=2\alpha R/4$	$R_{b,1}=0$
2	$R_{a,2}=2\alpha R/4$	$R_{b,2}=2(1-\alpha)R/2$
3	$R_{a,2}=2\alpha R/4$	$R_{b,2}=2(1-\alpha)R/3$
4	$R_{a,2}=2\alpha R/4$	$R_{b,2}=2(1-\alpha)R/4$
5	$R_{a,1}=2\alpha R/4$	$R_{b,2}=2(1-\alpha)R/5$
6	$R_{a,2}=2\alpha R/4$	$R_{b,2}=4(1-\alpha)R/6$
7	$R_{a,1}=2\alpha R/4$	$R_{b,2}=4(1-\alpha)R/7$
8	$R_{a,2}=2\alpha R/4$	$R_{b,2}=4(1-\alpha)R/8$

表 5　矿池收益矩阵 2

Table 5　Miner's reward matrix 2

状态	矿池 A	矿池 B	概率 P
s_1	$\frac{2}{M}\alpha KR$	$\frac{2(k-1)}{N}(1-\alpha)KR$	$\frac{M-j-1}{M-1}$
s_2	$\frac{2}{M}\alpha KR$	$\frac{2(k-1)+1}{N}(1-\alpha)KR$	$\frac{1}{M-1}$
s_3	$\frac{2}{M}\alpha KR$	$\frac{2k}{N}(1-\alpha)KR$	$\frac{j-1}{M-1}$

定理 2：

当 $1\leq j<\frac{M}{2}$ 时，若 $0<\alpha<\frac{1}{2}$，则当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}>1$ 时，池 A 为最优策略，当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}=1$ 时，池 A 与池 B 均为最优策略，当 $\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}<1$ 时，池 B 为最优策略。若 $\frac{1}{2}<\alpha<1$，则最优策略为池 A。

当 $\frac{M}{2}\leq j\leq M$ 时，若 $0<\alpha<\frac{1}{2}$，则当池 B 为最优策略。若 $\frac{1}{2}<\alpha<1$，则当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}>1$ 时，最优策略为池 A，当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}<1$ 时，最优策略为池 B，当 $\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}=1$ 时，池 A 与池 B 均为最优策略。

证明：

a)当 $\frac{M-j-1}{M-1}>\frac{j-1}{M-1}$ 时，即 $1\leq j<\frac{M}{2}$。

令 $R_1=\frac{R_{a,1}}{R_{b,1}}-1=\frac{N}{N-j}\cdot\frac{\alpha}{1-\alpha}-1$，当 $R_1>0$ 时，$R_{a,1}>R_{b,1}$，选择池 A。

b)当 $R_1<0$ 时，即 $R_{b,1}>R_{a,1}$，选择池 B。当 $R_1=0$ 时，$R_{a,1}=R_{b,1}$，池 A 与池 B 均为最优策略。当 $\frac{1}{2}<\alpha<1$ 时，$R_1>0$ 恒成立，故选择池 A。当 $0<\alpha<\frac{1}{2}$ 时，需要进一步计算 R_1 的值，从而作出相应的选择。

c)当 $\frac{j-1}{M-1}\geq\frac{M-j-1}{M-1}$ 时，即 $\frac{M}{2}\leq j\leq M$。

令 $R_3=\frac{R_{a,3}}{R_{b,3}}-1=\frac{N}{kM}\cdot\frac{\alpha}{1-\alpha}-1$，若 $R_3>0$，则 $R_{a,3}>R_{b,3}$，选择池 A。若 $R_3<0$，则 $R_{b,3}>R_{a,3}$，选择池 B。若 $R_3=0$，则

$R_{a,3}=R_{b,3}$，池 A 与池 B 均为最优策略。当 $0<\alpha<\frac{1}{2}$ 时，显然 $R_3<0$，选择池 B。当 $\frac{1}{2}<\alpha<1$ 时，需进一步计算，从而作出相应的选择。

由定理 1 和 2 可知，最优的矿池选择策略在以上讨论的两种情形下是相同，故在此不再详细举例。

2　仿真与分析

在本章中对所提出的矿池选择策略进行了评估。为了能更好的展现本文提出的策略的优劣，同时进行了对照实验，将总是选择矿池 A 称为 A 策略，总是选择矿池 B 称为 B 策略，本文提出的策略称为 New 策略。通过上章的讨论，使用最大期望值准则得出的选择策略，简单而言就是选择矿池算力较大的一方能够获增加矿工的期望收益。当矿池 A 和矿池 B 的算力相等时，显而易见，应选择矿池 A，因为矿池 A 的收益稳定性更好。为了能够直观地验证使用最大可能性准则得出的策略是否有效，进行了以下实验。

实验使用蒙特卡洛方法模拟挖矿过程，由 Python 编程语言实现，主要使用了 Numpy 科学计算库和 Matplotlib 绘图库。Numpy 库进行仿真实验，Matplotlib 绘图库将模拟结果以图表的方式展现。实验环境：Winows 7 64 位系统、Python3.6 工具。

2.1　实验设计

实验场景为在区块链网络中存在两个矿池 A 和 B，它们的算力分别为 α、β，矿池 A 和 B 分别采取的奖励分配机制为 Proportional、PPLNS。由 1.3 节的讨论得知在每个回合中提交一个或两个部分工作量证明的最优策略相同，故为了简单起见，本实验假设每个矿工在每个回合只能发送一个部分工作量证明，并且矿池 A 和 B 在每个回合中收到的部分工作量证明总数都为五个，矿池 B 每经过三个回合分发一次奖励，则 N 可能的取值为{1,2,...,15}，矿工所提交的部分工作量证明在全部工作量证明中的位置用 i 表示，$1\le i\le 5$。实验给出了当矿池 A 和 B 的算力分别为 $\alpha=0.45,\beta=0.55$、$\alpha=\beta=0.5$、$\alpha=0.55,\ \beta=0.45$ 以及对任意 $N=[1,2,\ldots,15]$ 的最优矿池选择策略。

2.2　结果分析

对于 N 的每个可能取值分别进行了 1 000 次实验，图 1 表示了在每个 N 可能取值的情形下矿工所提交部分工作量证明的在五个位置的次数分布。由于提交的部分工作量证明位置具有等可能性，所以可以观察到每个位置的部分工作量证明个数为 200 左右。对应于每个 N 可以分为两种状态 s1、s2，图 2 表示了对于每个 N 的取值，在 1 000 次实验中所属两种状态的次数。

图 3~5 分别表示了当矿池 A 和 B 的算力在不同情况下对应的最优选择策略。可以看出，当 N 取值相同时，由于矿池 A 和矿池 B 算力的不同，最优选择策略也会发生相应改变。当矿池算力一定时，最优选择策略同样受到 N 取值的影响。

可以得出结论：

a)当 $\alpha=0.45,\beta=0.55$ 时，对于 N={1,2,8}，矿工的最优策略为选择矿池 A；对于 N={3,4,5,6,7,9,10,11,12,13,14,15}，矿工的最优策略为选择矿池 B。

b)当 $\alpha=\beta=0.5$ 时，对于 N={1,2,6,7,11,12}，最优策略为矿池 A；对于 N={3,4,8,9,13,14}，矿工的最优策略为选择矿池 B；对于 N={5,10,15}，矿池 A 和矿池 B 均为最优策略。

c)当 $\alpha=0.55,\beta=0.45$ 时，对于 N={3,4,8}，矿工的最优策略为选择矿池 B；对于 N={1,2,5,6,7,9,10,11,12,13,14,15}，矿工的最优策略为选择矿池 A。

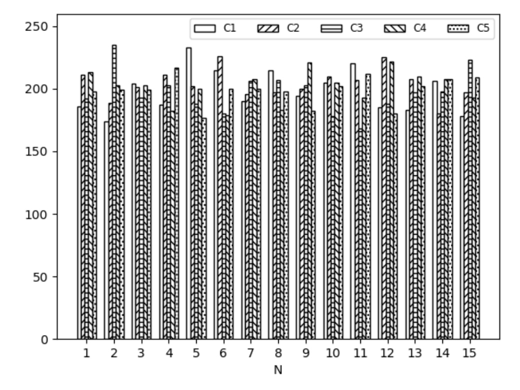


图 1　对应每个 N 的五种情况次数

Fig. 1　Corresponds to five cases of each N

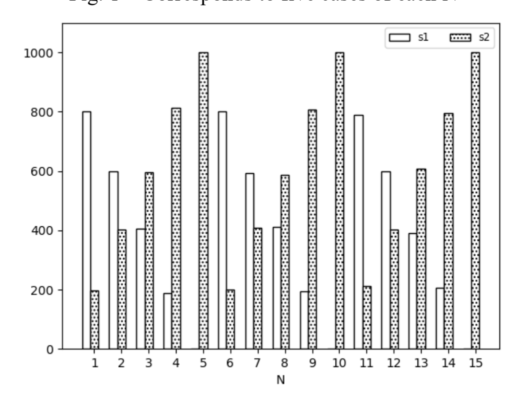


图 2　对应每个 N 的两种状态次数

Fig. 2　Corresponds to the number of states of each N

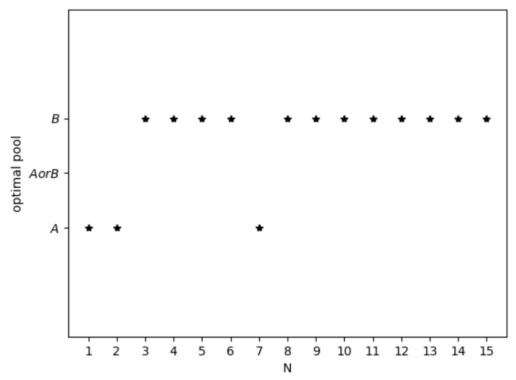


图 3　$\alpha=0.45$ $\beta=0.55$ 时的最优策略

Fig. 3　Optimal pool selection strategies for miner under $\alpha=0.45$ $\beta=0.55$

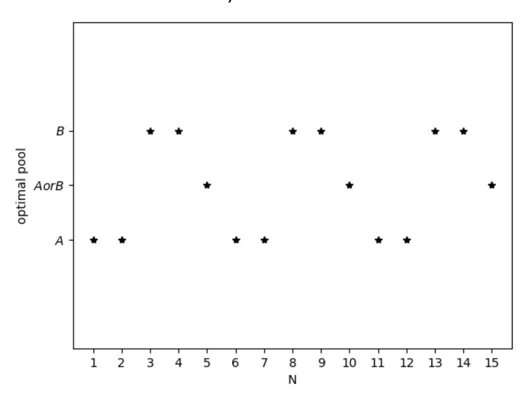


图 4　$\alpha=\beta=0.5$ 时的最优策略

Fig. 4　Optimal pool selection strategies for miner under　$\alpha=\beta=0.5$

通过比较在 1 000 次实验中矿工采取 New 策略获得的收益与采取 A、B 策略获得收益，可以得出 R(New)<R(A),

R(New)>R(A)和 R(New)<R(B)，R(New)>=R(B)的次数，如图 6~8 所示。对于三种不同的矿池算力情形以及任意 N 的情况，在 1 000 次实验中，矿工采取 New 策略获得的收益在绝大多数情况下都要高于采取单一 A、B 策略获得的收益，说明 New 策略要优于单一策略。

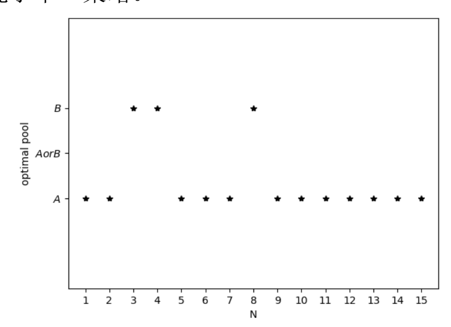


图 5　$\alpha=0.55$ $\beta=0.45$ 时的最优策略

Fig. 5　Optimal pool selection strategies for miner under　$\alpha=0.55$ $\beta=0.45$

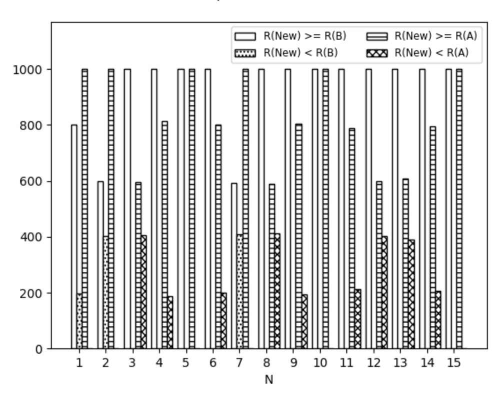


图 6　$\alpha=0.45$ $\beta=0.55$ 时策略优劣比较

Fig. 6　Strategy comparison under　$\alpha=0.45$ $\beta=0.55$

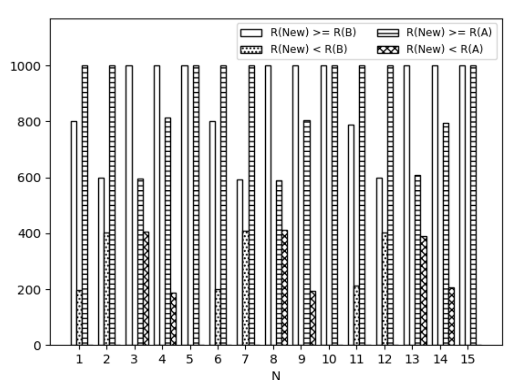


图 7　$\alpha=0.5$ $\beta=0.5$ 时策略优劣比较

Fig. 7　Strategy comparison under　$\alpha=0.5$ $\beta=0.5$

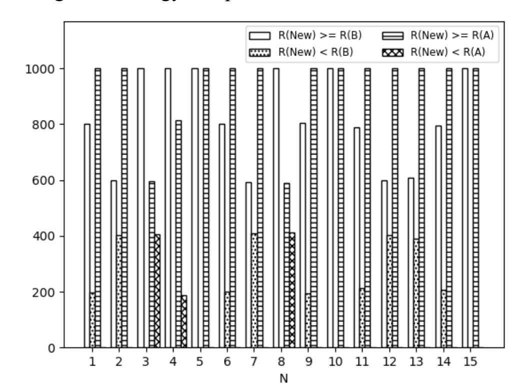


图 8　$\alpha=0.55$ $\beta=0.45$ 时策略优劣比较

Fig. 8　Strategy comparison under $\alpha=0.55$ $\beta=0.45$

3　结束语

本文研究了区块链网络中矿池选择的问题。考虑了在区块链网络中具有竞争关系，并且采取不同奖励分配系统的矿池对矿工收益的影响，分别使用最大可能性准则和最大期望值准则进行了研究与分析，并给出了针对不同矿池算力时的最优选择策略。同时设计了相应的实验来评估所提出的矿池选择策略，实验结果表明了所提出矿池选择策略的有效性。

但本文的研究仍有不足之处：没有考虑当一个回合中矿池所收到的工作量证明个数不同时的因素，以及当矿池算力不恒定时的情况。

针对以上待解决的问题，提出了可能的解决思路：在一个回合中，矿池内工作量证明的产生个数只与节点算力和部分工作量证明难度两个因素有关，并且假设整个区块链网络的总算力恒定不变，可设置两个参数 $\varepsilon_1,\varepsilon_2$ 分别表示两个矿池间的迁移率，根据算力大小以及部分工作量证明难度可以得出在单位时间内生成部分工作量证明的个数。由于产生工作量证明的过程是一个随机过程，所以可以使用蒙特卡洛方法模拟挖矿过程，利用风险决策方法进行分析。

参考文献：

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008) [2018-9-13]. https://bitcoin. org/bitcoin. pdf.

[2] 袁勇，王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报，2016, 42 (4): 481-494. (Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42 (4): 481-494.)

[3] 李董，魏进武. 区块链技术原理、应用领域及挑战 [J]. 电信科学，2016, 32 (12): 20-25. (Li Dong, Wei Jinwu. Theory, application fields and challenge of the blockchain technology [J]. Telecommunications Science, 2016, 32 (12): 20-25.)

[4] Eyal I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities [J]. Computer, 2017, 50 (9): 38-49.

[5] 祝烈煌，高峰，沈蒙，等. 区块链隐私保护研究综述 [J]. 计算机研究与发展，2017, 54 (10): 2170-2186. (Zhu Liehuang, Gao Feng, Shen Meng, *et al.* Survey on privacy preserving techniques for blockchain technology [J]. Journal of Computer Research and Development. 2017, 54 (10): 2170-2186.)

[6] 刘敖迪，杜学绘，王娜，等. 区块链技术及其在信息安全领域的研究进展 [J]. 软件学报，2018, 29 (7): 2092-2115. (Liu Aodi, Du Xuehui, Wang Na, *et al.* Research progress of blockchain technology and its application in information security [J]. Journal of Software, 2018, 29 (7): 2092-2115.)

[7] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications [C]// Proc of International Conference on the Theoryand Applications of Cryptographic Techniques. Berlin: Springer, 2015: 281-310.

[8] Lewenberg Y, Bachrach Y, Sompolinsky Y, *et al.* Bitcoin mining pools: a cooperative game theoretic analysis [C]// Proc of the 14th International Conference on Autonomous Agents and Multiagent Systems. Richland: IFAAMAS, 2015: 919-927.

[9] Fisch B, Pass R, Shelat A. Socially optimal mining pools [C]// Proc of the 13th International Conference on Web and Internet Economics. Berlin: Springer, 2017: 205-218.

[10] Rosenfeld M. Analysis of Bitcoin pooled mining reward systems

[EB/OL]. (2011) [2018-10-23]. https://arxiv. org/abs/1112. 4980.

[11] Liu Xiaojun, Wang Wenbo, Niyato D, *et al.* Evolutionary game for mining pool selection in blockchain networks [J]. IEEE Wireless Communications Letters, 2017, 7 (5) , 760-763.

[12] Qin Rui, Yuan Yong, Wang Feiyue. Research on the selection strategies of blockchain mining pools [J]. IEEE Trans on Computational Social Systems, 2018, 5 (3): 748-757.

[13] Eyal I. The miner's dilemma [C]// Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2015: 89-103.

[14] Luu L, Saha R, Parameshwaran I, *et al.* On power splitting games in distributed computation: the case of bitcoin pooled mining [C]// Proc of the 28th IEEE Computer Security Foundations Symposium, Piscataway, NJ: IEEE Press, 2015: 397-411.

[15] Heilman E. One Weird trick to stop selfish miners: fresh bitcoins, a solution for the honest miner (poster abstract) [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 161-162.